

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

)	
)	
UNITED STATES OF AMERICA)	
)	
v.)	CRIMINAL NO. 21-cr-10104-PBS
)	
VLADISLAV KLYUSHIN)	
Defendant)	
)	
)	

**REPLY MEMORANDUM FURTHER SUPPORTING
MOTION TO ACQUIT FOR IMPROPER VENUE**

Par for the course it has followed throughout this prosecution, the government’s Rule 29 opposition is long on bluster but strikingly short on substantive engagement. Unable to rescue its phantom venue case on the merits, the government aims to distract the Court by pretending Vladislav Klyushin’s trial never happened – and conjuring a wishful one its lawyers have lately come to prefer.¹ Regrettably for the government, the decoy succeeds only in leaving the pivotal facts undisputed, with the inexorable consequence: dismissal of the indictment for want of venue.

Among those pivotal facts the government vainly seeks to wave off – and thus implicitly concedes by freighted silence:

1. The Court expressly instructed Klyushin’s jury – over vehement government objection – to “consider” as to venue “the nature of the crime[s] alleged and identify the[ir ...] essential conduct elements” (counts One through Four) and determine whether the conspiracy’s

¹ See? Two can play at wordsmithing. *Cf.* Dkt. 225 at 2 (making the shoe-on-other-foot accusation that Klyushin “whistles past the venue evidence” presented at trial).

“essential conduct elements took place” abroad (Count One).² Those instructions are law of the case for purposes of this motion, and they control its disposition.³ It’s far too late in the day for the government to rehash its failed objections and make believe the Court is writing on a blank slate.⁴

2. By the same token, the Court’s instructions cogently distilled for the jury the essential conduct elements⁵ of the charged hack-and-trade scheme – the ineluctable crux of all four indictment counts – pointedly saying they “involved” Klyushin or a confederate “misrepresenting” their “identity online to access computer systems to obtain material nonpublic information to trade on the confidential information.”⁶ Having sought and gained that charge⁷ – consigned to a single collateral flyby in the government’s 21-page submission – over defense

² 2/10/23 T. 136, 138.

³ The government falls flat in urging the Court to analyze Count Four under the discrete statutory venue provision for securities fraud. Dkt. 225, *e.g.*, 4, 14-16. To the contrary, it was *Klyushin* who unavailingly raised that provision at trial in resisting the generalized venue instructions – applicable to all four counts – pressed by the *government*. *Compare id.*, *e.g.*, 140 at 28-29 with *id.* 196 at 3 (Klyushin noting that “Count Four (securities fraud) has its own statutory venue provision, supplanting both [18 USC] §§ 3237 and 3238 as to that charge”) (citing *US v. Royer*, 549 F.3d 886, 893-94 (CA2 2008)). It follows that the government has long since forfeited, if not affirmatively waived, its afterthought of an effort to coopt the defense’s venue position on Count Four.

⁴ *See* Dkt. 225, *e.g.*, 4-5, 7-11 (“even if the Court were to conclude [sic] that venue over the hacking offense depends on a determination of where the essential conduct elements of that crime lie”), 14-17, 20 (§ 3238 “satisfied [sic] without regard to where ... essential conduct elements of ... crimes [begun abroad] were committed”) (citation omitted).

⁵ Though the government renews its trial bid to blur the two (Dkt. 225, *e.g.*, 11-12), essential *conduct* elements remain different from – and narrower than – essential *offense* elements. *Id.* 222 at 2 & n.6 and authorities cited.

⁶ 2/10/23 T. 129-30.

⁷ *E.g.*, Dkt. 140 at 12, 20.

objection,⁸ the government can hardly back away from it now. Much less could it do so credibly, as the government drew the charge directly from *Dorozkho*⁹ and *Khalupsky*,¹⁰ the vaunted conceptual models for Klyushin’s prosecution.¹¹

3. Far from integral to the essential offense conduct – accessing protected computers and obtaining confidential information by misrepresenting identity – the use of an IP address ostensibly traced to Boston, MA was purely coincidental. Indeed, the government cannot – and does not – plausibly deny that Beantown played nothing more than a bit part or cameo role in this case: one of a chance locale that allegedly happened to associate to an intermediate IP address *assigned at random* by a Virtual Private Network (VPN).¹²

After all, the record shows that the operative VPN, Strong, didn’t advertise or provide a status for any Boston-based servers in Sep. 2018 or Mar. 2019 – the periods immediately before and shortly after the late Oct. and early Nov. DFIN intrusions.¹³ Nor was there evidence that Klyushin or any putative coconspirator signed up for or used any services of StackPath, the

⁸ Compare Dkt. 225 at 15 (gaslighting assertion that Klyushin “concedes” this “instruction w[as] correct”) with, e.g., *id.* Nos. 96, 103, 141 at 26 & n.23, 154 at 4-5 (defense strenuously contesting validity of underlying prosecution theory, and vigorously protesting propriety of corresponding jury instruction, from case’s onset); cf., e.g., *id.* 222 at 1 n.1 (“expressly” reserving for appeal all “dismissal and acquittal arguments made before and during trial”).

⁹ *SEC v. Dorozkho*, 574 F.3d 42 (CA2 2009).

¹⁰ *US v. Khalupsky*, 5 F.4th 279 (CA2 2021), *cert. denied*, 142 S. Ct. 761 (2022).

¹¹ E.g., *US v. Klyushin*, Criminal Action No. 21-10104-PBS, __ F. Supp. 3d __, 2022 WL 17983984, at *3 (D. Mass. Dec. 2, 2022).

¹² See Dkt. 222 at 3 & n.11.

¹³ Ex. 176, 2/7/23 T. 24-25, 2/9/23 T. 37.

company that ultimately subleased the relevant IP block¹⁴ – let alone that they selected Boston as the server location to use. On this record, in fact, *no one* using Strong VPN at the time would have known that it connected them to a server based in Boston.

While the government quibbles over semantics,¹⁵ then, its intricate verbal gymnastics¹⁶ can't obscure the bottom line: there is not a shred of proof that Klyushin or his supposed criminal partners "purposely availed themselves of a Boston-based IP address or consciously actuated its use."¹⁷ Even better, there's not a shred of proof they did *anything* – that they took *any* step whatever – to actuate such use: consciously, purposely, foreseeably or otherwise. And as deployed in this case, the statutes at hand – by their essential terms – "punish[] only the *actions* ... [a] defendant takes to access and obtain" off-limits information from a protected computer.¹⁸

¹⁴ 2/7/23 T. 21.

¹⁵ Dkt. 225 at 8 ("it matters little whether Klyushin used the Boston server as a 'pass through'" – a term lifted from the government's own manual for prosecuting computer crime – "or as the launching point [sic] for his improper use of Julie Soma's credentials to access DFIN's servers"). More on the manual later.

¹⁶ *Ibid.*, e.g., 10 (attempting to misdirect the Court with the odd and extraneous truism that conspirators "did not need Soma's username and password to access the Boston server" – never charged as a protected computer or hacking victim here – "from Russia"), 15-16 (similar), 11 (couching "Boston IP address []as the locus [sic] from which the schemers transmitted interstate wires to DFIN for the purpose of accessing its servers, and to which they received wires from DFIN transmitting stolen MNPI"), 12 (first full paragraph, particularly word salad Clause (2)), 13 (styling "transmission of Soma's credentials from Massachusetts to DFIN's computers in Illinois" as offense "gravamen" [sic]), 17 (insisting schemers "*used*" [sic] Boston server to "transmit" Soma credentials to DFIN servers and gain unauthorized access to MNPI, "which they then viewed and *downloaded back to the Boston server*" [sic]) (emphasis ours).

¹⁷ Dkt. 222 at 3.

¹⁸ *US v. Auernheimer*, 748 F.3d 525, 537 (CA3 2014) (emphasis supplied); *see also id.* 533 (identifying offense conduct's essential "nature" by reference to government's indictment and trial presentation).

In stark contrast, any Boston connection here was entirely fortuitous. For all it mattered to Klyushin, his reputed cohorts or any other purported Strong or StackPath user, any intermediate server or IP address might – and just as well could – have resolved to Toledo, Tokyo or Timbuktu. More precisely, they could have resolved to *anywhere* – or at least anywhere in the United States – to successfully carry out the scheme *as framed by the government itself*.¹⁹ Their arbitrarily linking to Boston instead thus epitomizes a circumstance element – simply a fact that existed at the time the defendants performed the criminal acts constituting the offense – that cannot establish venue as a matter of law.²⁰ And, concomitantly, it’s the very antithesis of the essential offense conduct our law requires.²¹

4. Cementing this conclusion is the Third Circuit’s *Auernheimer* opinion, the closest reported factual case to Klyushin’s – and a decision that demolishes the government’s tortured venue theory. So, unsurprisingly, the government addresses *Auernheimer* only by mangling its logic and holding beyond recognition.²²

Though you wouldn’t know it from the government’s rosy spin, *Auernheimer* **rejected** substantially the same argument its lawyers peddle here. Venue in cases like this one, the Third

¹⁹ See Dkt. 225, e.g., 12 (alleging “VPN server ... ma[d]e it appear that the access to DFIN’s computer network was coming from a *domestic source*”) (emphasis ours), 16 (contending schemers strove to “hide their tracks and make it difficult to trace the hacks back to Russia”), 18 (claiming the “*whole purpose* of using anonymizing VPNs was to hide the schemers’ location from their victims while lulling DFIN and TM into believing that the access to their networks was coming from legitimate sources *within the United States*”) (second emphasis ours).

²⁰ Dkt. 222 at 2 & n.6 and authorities cited.

²¹ Nor, for similar and constitutional reasons outlined in our moving papers, did any essential Count One conspiratorial *conduct* occur abroad for high-seas venue purposes. *Ibid.* 6-7 & sources cited.

²² Compare Dkt. 225 at 8, 11-12 with 748 F.3d at, e.g., 531.

Circuit thus ruled, appropriately resides – *even for a conspiracy charge*²³ – in the districts where the targeted “servers” are “located” and duplicitously “accessed” – but *not* in those where “[n]o protected computer [i]s accessed and no data ... obtained.”²⁴ As *Auernheimer* explained, that’s because the “essential conduct elements” at issue comprise nothing more than “*accessing* without authorization and *obtaining* information.”²⁵

Accordingly, since DFIN’s and Toppan Merrill’s protected computers weren’t located in Boston²⁶ – and access wasn’t “initiate[d]” or information “obtained” there²⁷ – *Auernheimer* dismantles the government’s position on venue. Specifically, “[b]ecause neither” Klyushin “nor [any] co-conspirator *performed* any ‘essential conduct element’ of the underlying ... violation[s] or any overt act in furtherance of the conspiracy” in Massachusetts, *Auernheimer* dictates that venue in this district was demonstrably “improper.”²⁸ Even more salient for Rule 29 review, it teaches that a jury correctly “instructed on venue ... *could not* have [reasonably] returned a guilty verdict” on this set of facts, perceiving “*no possibility*” that *any* rational “jury could have found venue proper.”²⁹ And again, the government reckons with this devastating precedent only by turning the case’s outcome – reversal for venue’s absence – on its proverbial head, somehow

²³ *Cf.* Dkt. 225 at 7-8.

²⁴ 748 F.3d at 533-34.

²⁵ *Ibid.* 533 (footnote omitted).

²⁶ *See* Dkt. 225 at 12.

²⁷ 748 F.3d at 533 n.3.

²⁸ *Ibid.* 535 (emphasis supplied); *accord id.* at 540 (similar).

²⁹ *Ibid.* 540, 541 n.9 (emphasis supplied).

managing to claim *Auernheimer* stands for the opposite of what it actually held.³⁰ That take is fanciful, straining all credulity.³¹

5. Try as it might, the government also can't escape or renounce the ultimate conclusions of its own manual for prosecuting computer crime: (A) prosecutors "looking to fix venue in the locale through which communications passed" should examine the facts "closely," and (B) where, as here, "the path of transmission is unpredictable, a court may find it *difficult to conclude that a crime was committed in a district merely because packets of information happened to travel through that district.*"³²

By choosing to prosecute Klyushin in Boston – rather than the Illinois site of DFIN's servers³³ or wherever Toppan's protected computers physically reside – the government

³⁰ See Dkt. 225 at 8, 11-12.

³¹ To the extent the government insinuates that "courts in this ... Circuit[] have expressly rejected" *Auernheimer* (*ibid.* 2), its memo fails to substantiate that suggestion. In fact, research reveals no authority within the First Circuit even citing – never mind "reject[ing]" – *Auernheimer*. Better yet, we have found no case in *any* jurisdiction disapproving *Auernheimer* in even remotely analogous factual circumstances. *Cf. US v. Mackey*, No. 21-CR-80 (NGG), 2023 WL 363595, at *9 (EDNY Jan. 23, 2023) (finding *Auernheimer*'s facts "easily distinguishable" in that it was "reasonably foreseeable that Tweets from a Manhattan-based Twitter personality with thousands of followers ... would reach or pass through a judicial district as large as the Eastern District of New York").

³² Dkt. 222 at 4-5. In its opposition, the government continually argues that valuable MNPI was "downloaded" to the Boston server. *See ante* n.16; Dkt. 225 at 8 (arguing that intruders engaged in "downloading valuable MNPI back to the Boston server for distribution to the conspirators..."). There was no evidence that any MNPI was stored on the Boston servers or stored on the Boston servers and then later disseminated to coconspirators. The government's argument fundamentally misunderstands how VPNs work. The Boston server passed electronic signals, but it did not store any information, including the alleged MNPI in this case. The server was not controlled by coconspirators. It was just one point (of the likely hundreds of others) that electronic information passed through to get from the DFIN server to the computer belonging to the alleged intruder.

³³ Dkt. 225 at 10 n.1, 12, 13.

heedlessly replicates the latter scenario, recklessly courting danger.³⁴ The government – not Klyushin – thus created and brought this venue headache on itself, by opting to proceed at its peril. To put it more bluntly, the whole venue mess amounts to a classic unforced error or self-inflicted wound, akin to an own goal in soccer or hockey. And, notably, the DOJ manual reached its conclusions having explicitly considered³⁵ the prospect of venue being “proper in any district through which electronic communications in furtherance” of a fraud scheme “pass”³⁶ – an argument the government blithely doubles down on here.³⁷

Faced with this body blow from their own superiors in the nation’s capital, the prosecutors can only resort to floating red herrings and attacking straw men. No matter. Who on earth ever suggested, for example, that the manual confers enforceable substantive or procedural rights?³⁸ Certainly not Klyushin. Rather, the venue guarantee derives from both constitutional – Art. III, § 2, Cl. 3 and the Sixth Amendment – and statutory – Criminal Rule 18 – sources.³⁹ The manual merely illustrates the guarantee’s proper implementation in cases like this one – exactly what *Auernheimer* cited and relied on it for.⁴⁰

³⁴ *Cf. Smith v. US*, No. 21-1576, Oral Argument T. 52 (U.S. Mar. 28, 2023) (“Why was this case brought in the Middle District of Florida [sic] – I mean, everyone seemed to – *you were alerted pretty early on that wasn’t the right venue.*”) (GORSUCH, J.) (emphasis supplied), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2022/21-1576_1b82.pdf (last visited Apr. 10, 2023).

³⁵ Dkt. 222 at 5.

³⁶ Dkt. 225 at 8.

³⁷ *Ibid.* 8, 9, 13, 16-17.

³⁸ *Cf. ibid.* 2, 12.

³⁹ *Auernheimer*, 748 F.3d at 532.

⁴⁰ *Ibid.* 533.

And whose fault is it that the government hasn't seen fit to update the manual – still its latest, most authoritative and definitive guidance on prosecuting computer crime – in what its lawyers call 13 years?⁴¹ Again, certainly not Klyushin.

6. In the end, the government's conception of venue is even more expansive than our moving papers gave it credit for.⁴² If its counsel had it their way, the government could bring criminal charges in *any* of the 94 federal judicial districts⁴³ “within the United States” where somebody incidentally happens to “access[]” one of the country's tens of thousands of “VPNs”.⁴⁴ something millions of people all over the world do every single minute of every single day – often by automated, unwitting default – for wholly innocuous, completely routine and entirely legitimate purposes.⁴⁵ That sort of breathtaking dragnet is a recipe for forum shopping, giving free rein to prosecutors' whims.⁴⁶

⁴¹ See Dkt. 225 at 12.

⁴² See Dkt. 222 at 7 (charging government would “prosecute in any district it chooses any foreign national whose conduct significantly touches, substantially impacts and largely takes place within identifiable districts in the United States”).

⁴³ https://en.wikipedia.org/wiki/United_States_federal_judicial_districts (last visited Apr. 10, 2023).

⁴⁴ Dkt. 225 at 12, 18.

⁴⁵ See 2/9/23 T. 19-20.

⁴⁶ See Dkt. 222 at 5-6, 7; *cf. Smith* Arg. T. 49-50 (“Well, how many times does the government, for example, get to either mistake or deliberately sue in the wrong district? You can imagine a situation, perhaps a rare one, but you can imagine it, where what's involved is an *abuse of their right to charge whatever they want*, not out of the blue, but in any case – many cases, like, take *internet crimes* and things like that, *there must be dozens of places where the government could charge, and why don't they just start with one and go through and wear down the defendant?*”) (ROBERTS, C.J.) (emphasis supplied); *id.* 51 (“it is an imposition on the defendant to have to litigate with the government, whether or not his, you know, vacation trip to wherever was enough to establish venue there”) (ROBERTS, C.J.).

While no doubt expedient for the *government*, demoting such a vital “protection for the *defendant*” to some second-class “technicality” – a pesky inconvenience – is impossible to square with the “fundamental” and “extraordinarily important” limits the constitution puts on “venue.”⁴⁷ Indeed, the “proper place of colonial trials was so important to the founding generation that it was listed as a grievance in the Declaration of Independence”⁴⁸ – reason enough to grant Klyushin’s motion and dismiss the indictment.

Respectfully Submitted,

Vladislav Klyushin,
By His Attorney,

/s/ Maksim Nemtsev
Maksim Nemtsev, Esq.
Mass. Bar No. 690826
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700
menemtsev@gmail.com

/s/ Marc Fernich
Marc Fernich
Law Office of Marc Fernich
800 Third Avenue
Floor 20
New York, NY 10022
212-446-2346
Email: maf@fernichlaw.com

Dated: Apr. 10, 2023

⁴⁷ *Auernheimer*, 748 F.3d at 532, 540 (emphasis supplied) (citation omitted).

⁴⁸ *Ibid.* 540 (citation omitted).

CERTIFICATE OF SERVICE

I, Maksim Nemtsev, hereby certify that on this date, Apr. 10, 2023, a copy of the foregoing documents has been served via Electronic Court Filing system on all registered participants.

/s/ Maksim Nemtsev
Maksim Nemtsev, Esq.